PC.NGO/70/10
14 September 2010

Organization for Security and Co-operation in Europe
Secretariat

ENGLISH only

Conference Services

OSCE Special Expert Meeting on Assessing the OSCE's Future Contribution to International Energy Security Co-operation

Vilnius, 13 – 14 September 2010

Session IV
Reliability of critical energy infrastructures

Presentation by Mr. Frank Umbach, Senior Associate & Head of the Programme "International Energy Security", CESS GmbH (Munich-Berlin)

Reliability of Critical Energy Infrastructures and New Security Challenges

OSCE-Special Expert Meeting on Assessing the OSCE‘s Future Contribution to International Energy Security Co-operation, Vilnius, 13-14 September, 2010

Dr. Frank Umbach

Senior Associate & Head of the Programme “International Energy Security”, CESS GmbH (Munich-Berlin)

E-Mail: Umbach@CESS-NET.EU

Introduction

- **Changing Conditions Since 2001: Increase of Security Threats to CEIP:**
  - **Attacks by:**
    - terrorist groups;
    - (transnational) crime organizations and groups
    - Private hackers;
    - Natural disasters.

Increasing Worldwide

  - **New Forms:**
    - Physical (attacking tankers, pipelines, refineries, electricity systems etc.);
    - **Cyber Threats as the Fifth Domain of Warfare:**
      - stealth, anonymity, unpredictability and lack of legal authority in the international law makes the attacker stronger than the defender.
      - Internet has blurred the lines between military and civilian strategies and targets.

Critical Energy Infrastructure Protection (CEIP) I

- **Cyber Threats:**
  - Attacks have risen in numbers and to an unprecedented level of sophistication
  - **Asymmetric Threat:** attacker have advantages by being better armed, can freely choosing the intensity of the attack as well as the target, no longer constraint by any geographical distances and frontiers as well as enjoying stealth, anonymity and inability to identify them;
  - **Botnet Threat "Conficker":**
    - infected 1.5 million computers,
    - able to function autonomously by recruiting and commanding 5 million computers in 122 countries;
    - Fear: coordinated simultaneous attacks on the economic system, critical national infrastructures, and the national defence structure of a country – all of them very interdependent of each other.
  - **Even protected *Infranets* of companies and ministries are not immune to cyberattacks as Pentagon officials admitted.**

CEIP II

- **Energy Spot Markets: Like Wall Street, dependent on the Computerization and the Worldwide Internet for Financial transaction:**
  - Manipulating energy spot and other energy market operations (e.g. Amsterdam Power exchange/APX, the Paris Powernext and the European Energy eXchange/EEX in Germany);
- **Western OECD-Countries: a Majority of CEI-Infrastructures Belong to the Private Industry (i.e. Germany: 85%):**
  - Need for PPP between governments/Ministries and the private industry as well as between private energy and other companies for strengthening CEIP.
- **World Economic Forum 2008:** 10-20% probability of a major breakdown of critical information infrastructure (CII) in the next 10 years, with a potential global economic cost of approximately 250 billion US$.

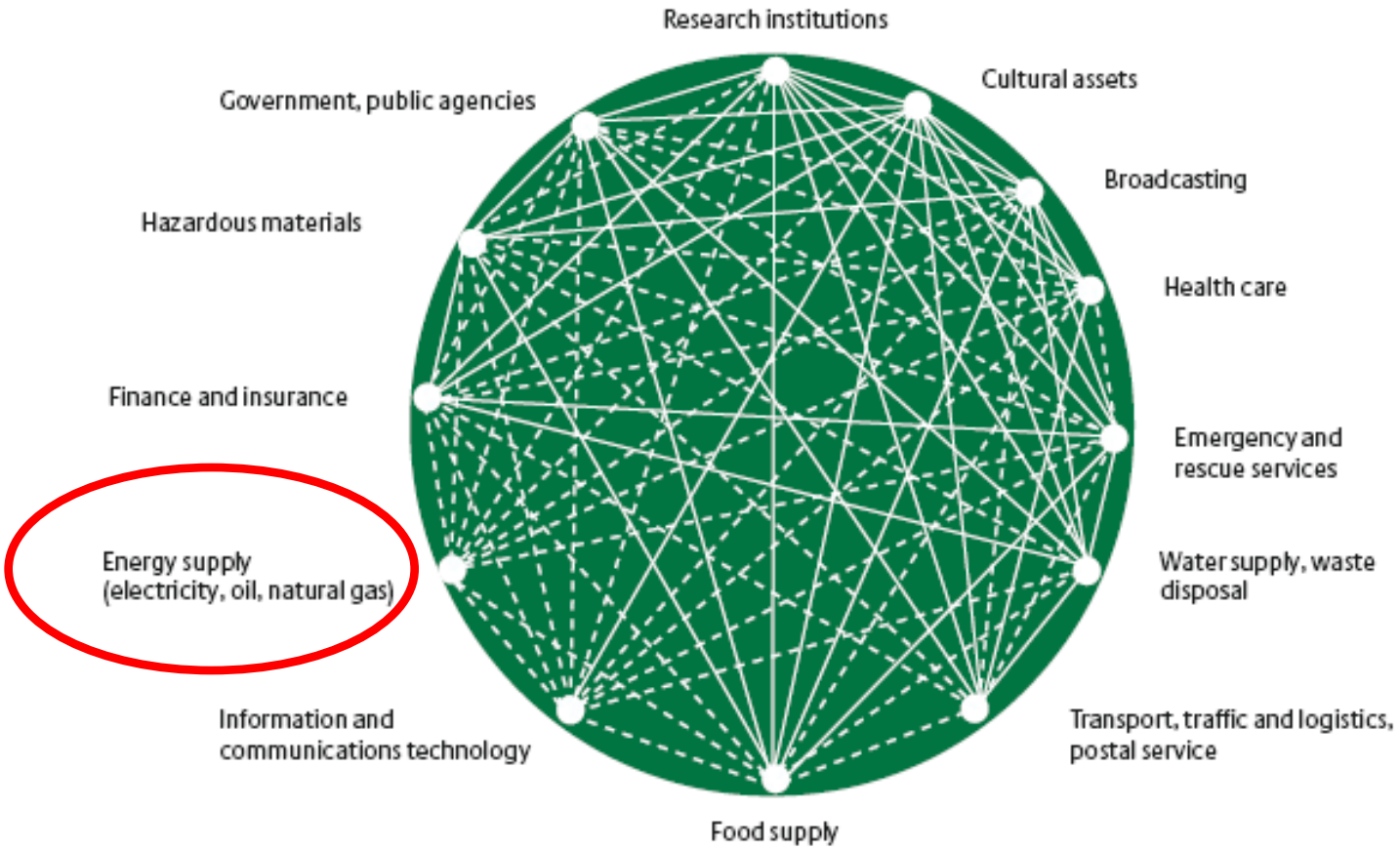
CEIP III

- **Cyberattacks:**
  - GB: responsible for shutting down the British House of Commons computer system in 2006 and attacks on networks of the British Foreign Ministry and other key departments in 2007;
  - India: Attacks on ministries, telecommunication centers/companies; armed forces and military institutions, embassies and consulates; encrypted diplomatic communication and NSC-Secretariat
  - Google and 30 other Leading High-Tech-Companies in the U.S.;
- **Professional Security & Risk Assessment Needs:**
  - physical and cyber security,
  - SCADA and data acquisition and distributed control systems (DCS),
  - communications security,
  - grid security,
  - distribution security,
  - generation security, and
  - nuclearbiological/chemical issues.

CEIP IV

- **Cascading Transborder Effects and Secondary Consequences**
  - **affecting image, reputation and performance of companies and governments) due to:**
    - dependence of almost all CEI on the availability of secure electricity supplies;
    - the revolutionary spread of ICT and Commercial of the Shelf(COTS)-products; and
    - the interlinkage of the different sectoral infrastructures and their specific vulnerabilities through electricity, ICT and SCADA systems.

Figure 1: Interdependencies of selected critical infrastructures



Source: Federal Ministry of the Interior (BMI), Protecting Critical Infrastructures – Risk and Crisis Management, Berlin, January 2008

Example: European Gas Infrastructure Security

- Major Challenge: Growing Security Requirements vs. Diminising Resources for Security Requirements;
- **Expanding Gas Infrastructure:**
  - New storage sites
  - LNG-terminals, ships and connecting pipelines (incl. addressing interrelated Maritime Security issues);
  - New gas interconnectors within the EU;
  - New pipelines between EU and producer countries (Russia, CACR, North Africa).
- **Reduced EU-Energy Demand and Fewer Pipeline Options:**
  - Reducing redundancy of potential infrastructure targets for terroririst attacks/cyber threats;
  - Fewer redundancy of potential infrastructure targets increases their strategic value for attacks and vulnerability for cascading transborder effects in gas and electricity supply (i.e. gas and electricity control centers, gas compressor stations etc.).

New Challenges of Energy Transportation Security I:

- Expanding length of transnational/interregional oil and i.p. gas pipelines in Europe and beyond;
- Global expansion of interregional gas trade/LNG transport and its specific vulnerabilities (incl. LNG-terminals);
- New gas and electricity interconnectors within the EU-27 (EC: March 2009) creating a new „*vulnerability paradox*“;
- **Expansion Integration and Synchronisation of the Intermeshed European Electricity Network Systems:**
  - **EU-27: new members into the *Union for the Coordination of Transmission of Electricity (UCTE)/now „European Continental Electrical Network (ENTSO-E);***
  - **Integration of RES;**
  - **Integration of Turkey and other non-EU-member („*Euro-Mediterranean Energy Market*“) as well as EU-member states (British Isles, Scandinavian and Baltic countries) into ENTSO-E;**

New Challenges of Energy Transportation Security II

- **Smart Grids and Supergrids:**
  - **will require quantitative and qualitative changes in the way electricity is moved within and between countries;**
  - **may create new frontiers by exploiting vulnerabilities for cyber attacks.**
- Liberalisation and Deregulation of Energy Policies in EU-27: up to 85% of CEI in member states belongs to private companies

  ⇒ need for PPPs and more governmental oversight and coordination.
- Power companies keep only few spare s of expensive generation parts, which can takes months to replace;

- **Effects and Impacts of New Transnational/Interregional Gas and Electricity Interconnectors in Europe-Eurasia-Mediterranean Region:**
  - National states more than ever linked with and dependent on each other‘s resiliency – and thus interdependent and mutually reinforcing;
  - Can both enhancing and decreasing national supply security;
  - Measures of CEIP only as strong a their weakest links

  ⇒ **need for collective transnational/interregional CEIP!**

New Security Challenges of Energy Control and Processing Systems

- **Energy Control Centers:**
  - have become a key element in the safe and secure operation of both installations and extended infrastructures;
- **Supervisory Control and Data Acquisition (SCADA):**
  - control the operation of power plants as well as of networks;
  - operation of huge border crossing gas networks require a network management & a control center hierarchy to ensure security of gas supplies;
  - security in process control systems is lagging 5-10 years behind the security of laptops or desktops.

Abbildung 4: *Typische SCADA Konsole*

Information- and Control Nerv-Centres being very vulnerable for potential cyber attacks.

Conclusions and Perspectives I

- Energy (i.p. electricity) is the lifeblood of modern, efficient societies and economies as well as of the secure functioning of all CI;
- Cross-border and cross-sector dependencies on CEI and ICT infrastructures are rapidly increasing and creating numerous new vulnerabilities;
- New security threats to CI emerge more quickly than policies and corporate security strategies are made to adopt;
- **Cyber Threats - the New Security Front:**
  - Increased communication and information flows - i.e. smart grids – will increase significantly cyber vulnerabilities;
  - Introducing smart grids: safety and security needs to be an integral part of the design criteria and adressed by companies and governments as the owners and operators of electric power grids;

Conclusions and Perspectives II

- **Potential Role of the OSCE:**
  - **Need for Re-Thinking, Conceptualizing and Coordination of Government and Corporate Energy Security Strategies:**
    - Business/Infrastructure Security as a main topic for defining a new balance between short-, mid- and long-term strategic interests of their demand and energy security concepts;
    - Recognizing safety and security as a competitive advantage in future oil, gas and electricity markets;
    - Pre-Condition: Need for functional integration of ***Energy Infrastructure Security*** in comprehensive demand and energy security concepts in corporate business and developments plans and company strategies;
    - Establishing newly defined working relationships with Govern-ments and International Organizations (i.e. EU, IEA, OSCE etc.);
    - Institutionalizing cooperation between Producer, Transit and Consumer States.
  - developing a "*Critical Energy Infrastructure Database*" (*CEID*), including on global attacks against CEI by terrorists and criminal organizations an d indiividuals (as suggested by *K.Rosner / F.Umbach in 02/10*).

Thank you very much for your attention!